F field

$F[x]$ polynomial ring

$f(x) \in F[x]$

$\downarrow$

irreducible

Let I be an ideal of $F[x]$ generated by f, i.e. $I = \langle f(x) \rangle$.

Thm: $F[x]/I$ is a field.

Pf: Consider a coset $g(x) + I$, $g(x) \neq 0$. So $\deg g < \deg f$.

Take the ideal J in $F[x]$ generated by $g(x)$ and $f(x)$, i.e.,

$$J = \{ g(x) h_1(x) + f(x) h_2(x) \mid h_1, h_2 \in F[x] \}$$

We know that J is principal so,

$$J = \langle r(x) \rangle$$

$\Rightarrow \quad f(x) = r(x)\, r_1(x)$

but $f(x)$ is irreducible so, either

$f(x) = c\,r(x)$ $\quad$ c is a constant $(c \neq 0)$

or $r(x)$ is a constant (not zero)

If $r(x)$ is a non-zero constant

$\Rightarrow \quad J = F[x] = \langle 1 \rangle$

$\Rightarrow \quad 1 = g(x)\, h_1(x) + f(x) h_2(x)$ for some $h_1, h_2 \in F[x]$

$\Rightarrow \quad 1 = g(x)\, h_1(x)$ in $F[x]/I$.

If $f(x) = c\,r(x)$

$\Rightarrow \quad J = I$

$\Rightarrow \quad g(x) \in I \Rightarrow g(x)$ is zero in $F[x]/I$

$\downarrow$

contradiction.

Can we compute this field explicitly?

F field (Char 0)

$F[x]$ polynomial ring

$f(x)$ irreducible polynomial

Suppose $f(\alpha) = 0$ for some $\alpha \in \mathbb{C}$

(α not necessarily in F)

<u>Definition:</u> We define $F[\alpha]$

$$= \left\{ a_0 + a_1\alpha + \cdots + a_n\alpha^n \;\middle|\; \begin{matrix} a_i \in F \\ n \in \mathbb{N} \end{matrix} \right\}.$$

1) $F \subseteq F[\alpha]$

2) $F[\alpha] \subseteq \mathbb{C}$

3) $F[\alpha]$ is a subring of $\mathbb{C}$.

<u>Thm:</u> $F[\alpha]$ is a field.

<u>Pf:</u> Let us define a map

$\varphi_\alpha : F[x] \to F[\alpha]$ as follows.

$$g(x) \longmapsto g(\alpha)$$

φ_α is a ring homomorphism.

<u>Claim:</u> $\ker \varphi_\alpha = \langle f(x) \rangle$

<u>Pf:</u> If $\varphi_\alpha(g) = g(\alpha) = 0$, we want to show that $g(x)$ is a multiple of $f(x)$.

<u>Observation:</u> If $h(\alpha) = 0$ and $h(x)$ is non-zero, then $\deg h(x) \geq \deg f(x)$

Suppose not, then we consider the set of polynomials

$$S = \left\{ h(x) \in F[x] \;\middle|\; \begin{array}{l} h(\alpha) = 0, h \neq 0 \\ \deg h < \deg f \end{array} \right\}$$

S is non-empty, so we can choose a polynomial $r(x) \in S$ of smallest degree.

By division algorithm

$$f(x) = r(x)\, q(x) + r_1(x)$$

Put $X=\alpha$ $\quad f(\alpha) = r(\alpha)\, q(\alpha) + r_1(\alpha)$

$f(\alpha) = 0 \;,\; r(\alpha) = 0$

$\Rightarrow \; r_1(\alpha) = 0$

$\Rightarrow \; r_1 = 0$, otherwise $r_1(x) \in S$ & $\deg r_1 < \deg r$ a contradiction.

$\Rightarrow \; f(x) = r(x)\, q(x)$

Since f is irreducible $\deg r = \deg f$ or r is a non-zero constant

$\downarrow$

Both give contradiction.

Finishing pf of the claim:

If $g(x)=0$, we are done, else $\deg g \geq \deg f$

$g(x) = f(x)\, q(x) + r(x)$

Put $X=\alpha$ $\quad \Rightarrow \; r(\alpha) = 0 \quad \Rightarrow \; r = 0$

So, g is a multiple of f.

$\Rightarrow$ $\operatorname{Ker} \varphi_\alpha \subseteq \langle f(x) \rangle$

$\langle f(x) \rangle \subseteq \operatorname{Ker} \varphi_\alpha$ follows because

$f(\alpha) = 0$.

So, $\operatorname{Ker} \varphi_\alpha = \langle f(x) \rangle$

$\text{Image } \varphi_\alpha = F[\alpha]$

By first isomorphism theorem

$$F[x] / \langle f(x) \rangle \cong F[\alpha]$$

$\downarrow$

field

So, $F[\alpha]$ is a field.

Examples

Example: 1) Evaluation at a point

F field $\quad \varphi_a : F[x] \longrightarrow F \qquad a \in F$

$$f(x) \longmapsto f(a)$$

$$\operatorname{Ker} \varphi_a = \langle x-a \rangle$$

$$\text{Image} = F$$

$$F[x] / \langle x-a \rangle \cong F$$

2) $\varphi_i : \mathbb{R}[x] \longrightarrow \mathbb{C}$

$$f(x) \longmapsto f(i) \qquad i^2 = -1$$

$$\operatorname{Ker} \varphi_i = \langle x^2+1 \rangle$$

$$\text{Image } \varphi_i = \mathbb{C}$$

$$\mathbb{R}[x] / \langle x^2+1 \rangle \cong \mathbb{C} = \mathbb{R}[i]$$

3) $f(x) = x^2 - 2 \in \mathbb{Q}[x]$

$$\mathbb{Q}[x] / \langle x^2 - 2 \rangle \cong \mathbb{Q}[\sqrt{2}]$$

Field Extensions / Intro to Galois theory

Defn: We say that L is a field extension of F is F is a subfield of L.

Examples:

$$\begin{array}{c} \mathbb{C} \\ | \\ \mathbb{R} \end{array} \qquad \begin{array}{c} \mathbb{C} \\ | \\ \mathbb{Q} \end{array} \qquad \begin{array}{c} \mathbb{R} \\ | \\ \mathbb{Q} \end{array}$$

$$\begin{array}{c} F(\alpha) \\ | \\ F \end{array}$$

$$\begin{array}{c} \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array} \qquad \begin{array}{c} \mathbb{Q}(i) \\ | \\ \mathbb{Q} \end{array} \qquad \cdots \qquad \begin{array}{c} \mathbb{Q}(\sqrt{d}) \\ | \\ \mathbb{Q} \end{array}$$

Consider two examples:

$$\begin{array}{c}\mathbb{Q}(\sqrt{2})\\ | \\ \mathbb{Q}\end{array} \qquad\qquad \begin{array}{c}\mathbb{Q}((2)^{1/3})\\ | \\ \mathbb{Q}\end{array}$$

$\sqrt{2}$ is a solution of $x^2-2=0$.

$(2)^{1/3}$ is a solution of $x^3-2=0$.

All the solutions of $x^2-2=0$ are

$\sqrt{2}, -\sqrt{2}$

$-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$

All the solutions of $x^3-2=0$ are

$(2)^{1/3}, \ \omega 2^{1/3}, \ \omega^2 2^{1/3}$.

$\omega 2^{1/3} \notin \mathbb{Q}(2^{1/3})$

Suppose it does.

$$\mathbb{Q}(2^{1/3}) = \mathbb{Q}[2^{1/3}]$$
$$= \{ q_0 + q_1 2^{1/3} + q_2 2^{2/3} \mid q_i \in \mathbb{Q} \}$$

If $\omega 2^{1/3} = q_0 + q_1 2^{1/3} + q_2 2^{2/3}$

$$\Rightarrow \omega = \frac{q_0 + q_1 2^{1/3} + q_2 2^{2/3}}{2^{1/3}}$$

is a real number

this is a complex number with non-zero imaginary part

Similarly $\omega^2 (2)^{1/3} \notin \mathbb{Q}(2^{1/3})$

$$\begin{array}{c} \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}$$ is an example of a <u>Galois</u> <u>extension</u>.

$$\begin{array}{c} \mathbb{Q}(2^{1/3}) \\ | \\ \mathbb{Q} \end{array}$$ is <u>not</u> a Galois extension.